Pattern Recognition for IT Security
Book of Abstracts

Workshop held in conjunction with DAGM 2010
Darmstadt, September 21, 2010

DAGM
Deutsche Arbeitsgemeinschaft für Mustererkennung e.V.

Fraunhofer IGD

TECHNISCHE UNIVERSITÄT DARMSTADT

Source: Wissenschafts- und Kongresszentrum Darmstadt GmbH & Co. KG

Preface

Graphical data, such as images or video streams, are of growing importance in several disciplines of IT security, ranging from biometric authentication over digital image forensics to visual passwords and CAPTCHAs. Consequently, methods of image analysis and pattern recognition are increasingly important to build security-critical applications. The aim of the workshop is to bring together researchers from the pattern recognition and security communities in order to exchange latest research results.

The workshop features papers on diverse topics, ranging from graphical authentication methods over biometrics to emerging research areas such as media forensics. We hope that the workshop stimulates the exchange of ideas between the security and pattern recognition communities and offers ample room for fruitful discussions.

Organization

Organizers

Stefan Katzenbeisser, Technische Universität Darmstadt
Jana Dittmann, Otto-von-Guericke-University Magdeburg
Claus Vielhauer, Brandenburg University of Applied Science

Program Committee

Jose L. Alba, University of Vigo
Jana Dittmann, Otto-von-Guericke University Magdeburg
Bernadette Dorizzi , Télécom Sud Paris
Stefan Katzenbeisser, Technische Universität Darmstadt
Ton Kalker, HP Labs
Matthias Kirchner, Technische Universität Dresden
Dominique Schröder, Technische Universität Darmstadt
Claus Vielhauer, Brandenburg University of Applied Science

Program

11.00 – 12.00 Alternative Authentication Methods

The IR Ring: Authenticating users' touches on a multi-touch display

Volker Roth, Philipp Schmidt, Benjamin Güldenring

Multi-touch displays are particularly attractive for collaborative work because multiple users can interact with applications simultaneously. However, unfettered access can lead to loss of data confidentiality and integrity. For example, one user can open or alter files of a second user, or impersonate the second user, while the second user is absent or not looking. Towards preventing these attacks, we explore means to associate the touches of a user with the user's identity in a fashion that is cryptographically sound as well as easy to use. We describe our current solution, which relies on a ring-like device that transmits a continuous pseudorandom bit sequence in the form of infrared light pulses. The multi-touch display receives and localizes the sequence, and verifies its authenticity. Each sequence is bound to a particular user, and all touches in the direct vicinity of the location of the sequence on the display are associated with that user.

CAPTCHAS: The Good, the Bad and the Ugly

Paul Baecher, Marc Fischlin, Lior Gordon, Robert Langenberg, Michael Lützow, Dominique Schröder

A CAPTCHA is a program that generates challenges that are easy to solve for humans but difficult to solve for computers. The most common CAPTCHAs today are text-based ones where a short word is embedded in a cluttered image. In this paper, we survey the state-of-the-art of currently deployed CAPTCHAs, especially of some popular German sites. Surprisingly, despite their importance and the large-scale deployment, most of the CAPTCHAs like the ones of the „Umweltprämie", the Bundesnetzagentur, and the Sparda-Bank are rather weak. Our results show that these CAPTCHAs are subject to automated attacks solving up to 80% of the puzzles. Furthermore, we suggest design criteria for „good" CAPTCHAs and for the system using them. In light of this we revisit the popular reCAPTCHA system and latest developments about its security. Finally, we discuss some alternative approaches for CAPTCHAs.

12.00 – 13.00 BIOMETRICS I

Security Enhanced Random Projection to Protect Biometric Templates

Bian Yang, Koen Simoens, Christoph Busch

We give in this paper an overview of the security concerns over random projection used for biometric template protection schemes under the token-stolen (or public parameter) case. Two security enhancing measures based on quantization are used to address these security problems. The first measure increases the computational complexity to search for the unprotected biometric features by the proposed quantization based dynamic projection matrix assembly mechanism. The second measure, as proposed in A. Nagara et al.'s work, is incorporated to thwart a genuine biometric feature estimation attack by a multi-level binarization. Extension of the projection matrix is also studied to improve the biometric performance. Experiments on the public database FVC2002DB2_A demonstrate the well-kept biometric performance of the proposed method under the security enhancing measures.

Analysis of Relative Entropy, Accuracy, and Quality of Face Biometric

Sabah A. Jassim, Hisham Al-Assam, Ali J. Abboud, Harin Sellahewa

The objectives of recent research efforts in biometric-based person identification has recently widened beyond improving accuracy of matching, to that of improving the security of biometric templates and by implication the security of cryptographic keys generated from biometrics. This paper aims to contribute to these recent objectives by investigating factors influencing accuracy rates and security of templates/keys from information theory point of view. We present an analysis of Relative Entropy (RE) measures for face biometric in relation to accuracy of face-based authentication. RE values of a user's biometric features is the amount of information that distinguishes the user from a given population. We shall establish that different feature extraction techniques (FET) have different RE values and compare RE values in PCA features with those for a number of wavelet subband features at different levels of decomposition. We shall demonstrate that for each of the FETs there is a strong positive correlation between RE and accuracy. Our analysis of the relation between accuracy and RE values show that except for the lowest image quality level, increased image quality results in increased RE and increased accuracy rate for all FETs. In fact, we observe that sever image quality degradation may result in more than 75% drop in RE vales in face images. The results confirm the superiority of wavelet-based FETs over PCA in terms of RE values and accuracy rates across different image quality levels. We also present a regional version of

these investigations in order to determine the facial features/regions that have more influence on accuracy and RE values. We also discuss the effect of individual differences on RE values and accuracy rates.

14.00 – 15.00 FORENSIC METHODS

Forensic Fingerprint Detection: Challenges of Benchmarking new Contactless Fingerprint Sensors - a first proposal

Marcus Leich, Michael Ulrich, Mario Hildebrandt, Stefan Kiltz, Claus Vielhauer

Latent contact-less fingerprint sensors are a very important lead in the forensic investigation of a crime scene. To be admissible in a court of law, the process and the technology used to locate, acquire and pre-process contact-less fingerprint data, must meet the "Federal Rules of Evidence". These include the question if the techniques and procedures have been tested. Contact-less approaches are currently emerging technologies. If this new technology is further developed, the proposed benchmarking framework helps to compare and rate different techniques according to their usefulness for investigating crime scenes.

A first approach for a benchmarking methodology scheme for contact-less fingerprint scanners (a detection device consisting of sensory equipment and the hard- and software components capable of locating, acquiring and pre-processing of image data) is presented. This methodology takes into account that different use-case scenarios such as "crime scene" and "forensic laboratory" impose different requirements on such a scanner. The presented framework is intended to assess the suitability of existing initial approaches and to serve as a guide for research and development of new approaches for pattern recognition and devices for contactless fingerprint scanning.

The benchmarking aspects proposed in this work include forensic legal requirements such as integrity, authenticity and confidentiality of the processed data and repeatability, which ensure the evidentiary value of the acquired data. Pattern recognition related aspects such as matching rates as well as the capability for separation of overlapping fingerprints and age detection are included. Since these aspects are highly dependent on the surface the fingerprint lifted from, these properties are measured for clearly defined objects and materials. To estimate the suitability for a given use-case scenario technical properties that include transportability, scan time, size of the measured surface, potentially hazardous effects on surrounding persons and materials as well as the robustness against environmental factors such as light, vibration, temperature and humidity are considered.

To aid research and development of new methods not directly performance relevant aspects such as the general type of the input sensory technology including the type of the acquired data (2D image, 3D height field, etc.) as well as the type of pre-processing algorithms employed are recorded. To demonstrate the application of this benchmarking scheme the performance of two existing off-the-shelf contact-less surface scanners is assessed for two different use-case scenarios. To support the development of new approaches, which conform to all of the aforementioned aspects, state-of-the-art research approaches are analysed with regard to the benchmarking aspects and proposals for future research are given.

First results indicate that further research into pattern recognition and improvements for sensor technology are required. The exemplary chosen and tested scanner systems lacked some of the forensic legal requirements, e.g. proof of authenticity, maintenance of a chain of custody. Also the sensory technologies need vast improvements to be able to investigate rough, uneven and absorbing surface materials. In pattern recognition, the ability to differentiate between overlap-ping fingerprints and putting them into sequence as well as mechanisms for age detection of fingerprints need to be extensively researched.

An ML Perspective on Feature-Based Forensic Camera Model Identification
Thomas Gloe, Nicolas Cebron, Rainer Böhme

State-of-the-art digital forensic techniques for camera model identification draw on machine learning (ML) to match characteristic features to specific camera models. This paper complements existing work, which is mainly focused on feature extraction and benchmarking, by three focused experiments related to design choices of the machine learning algorithm and its parameters. In particular, backward feature elimination finds 40 out of originally 57 features important; a comparison of approaches to detect whether a given image most likely stems from a camera model not included in the training shows a clear advantage of binary SVMs over one-class SVMs; testing model identification with scaled or grayscale images reveals a pretty good robustness against these classes of common transformations only if they are anticipated.

15.00 – 16.00 BIOMETRICS II

Effects of Aging Processes on Dynamic Biometric Handwriting

Tobias Scheidat, Juliane Heinze, Claus Vielhauer, Andrey Makrushin

In biometrics the variance between data acquired from the same user and same trait is not only based on differing sensors or day's form of the user, but it also depends on an aging factor. With the time the biological characteristics of a human body change, which leads to physical and/or mental alternations, which may have significant influence to the biometric authentication process. In order to parameterize a biometric system, the study of the degree of influence of the human aging is an important step. In this paper we provide an experimental evaluation on the influence of changes of handwriting biometrics by acquiring data from writers in two sessions at a distance of at least two years (long term database) and three sessions with a time difference of one month each (short term database). The aim is to provide evaluation results to analyse the potential impact of aging and aging processes on a biometric handwriting system in terms of authentication performance.

Selection of handwriting features for better user authentication via secure sketch algorithm

Andrey Makrushin, Tobias Scheidat, Claus Vielhauer

The feature extraction, which is the most critical part of biometric recognition systems, is solely done based on expert knowledge or rather intuitively. Thus, there is not any guaranty that extracted features are suitable to distinguish between registered and non-registered users. Moreover, the expert knowledge could be only applied for particular quality of raw data or defined only for one particular database. Therefore, the feature analysis is required to estimate the discrimination power of extracted features and automatically eliminate all irrelevant or redundant ones before the classification begins. In order to provide feature ranking and consequent filtering, authors suggest in this work several heuristics and compare these to each other. The experiments were done on features extracted from handwriting data. The secure sketch algorithm was used for user authentication. The evaluation results demonstrate the significant improvement of error rates when feature selection is provided. Furthermore, the lower number of features ensures the reduction of computational complexity and, thus, classification speed-up.

16.30 – 17.30 WATERMARKING AND STEGANOGRAPHY

Multi-level information fusion and model plausibility checking in the application of statistical pattern recognition in audio steganalysis

Christian Kraetzer, Jana Dittmann, Marcus Leich

In the paper we extend an existing information fusion based audio pattern recognition approach used in steganalysis by two different kinds of evaluations: First the enhancement of observations on fusion from considering only segmental features to combinations of segmental and global features, with the result of a reduction of the required computational complexity for testing by about two magnitudes while maintaining the same degree of accuracy. The second evaluation tries to build a basis for estimating the plausibility of the introduced audio steganalysis approach by observing the sensibility of models used in the pattern recognition on steganographic material against typical signal modification operations like de-noising or 128kBit/s MP3 encoding. Our results show that for some of the tested classifiers the probability of false alarms rises dramatically after such modifications.

Robust hash controlled watermark embedding

Martin Steinebach, Sascha Zmudzinski, Moazzam Butt

The process of embedding a digital watermark into a media file is often complex and time consuming as multiple operations take place within the process to ensure a high level of perceived quality of the marked copy and a high robustness of the embedded watermark. So far, improvements of the watermarking algorithms also lead to a higher complexity of the embedding process: State of the art watermarking algorithms require spectral transformation operations as well as windowing and perceptual models for masking the embedded watermark. Our new concept is to set up a collection of already computed watermarking signals and mix them with the cover signal for fast and simple embedding. To ensure that the watermark signal is well suited for the embedding position with respect to masking, we suggest using robust hash technology.